

FQ5-511

32

Claims:

1. A system comprising:

a participant subsystem that is authorized to anonymously participate in a plurality of sessions using secret information provided by a manager subsystem; and

5 a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session,

wherein

the participant subsystem comprises:

10 an anonymous signing section for authorizing individual data using the secret information depending on session-related information to produce anonymous participation data with anonymous signature, and

the reception subsystem comprises:

15 an anonymous signature determining section for determining whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem; and

20 a sender match determining section for determining whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

FOLEO 00000000

FQ5-511

33

2. The system according to claim 1, wherein the anonymous signature includes data that is generated by a predetermined expression using the session-related information and the secret information, wherein the sender
5 match determining section checks the data included in the anonymous signature of received anonymous participation data.

3. The system according to claim 2, wherein the predetermined expression is represented by raising a session-dependent base to a power that is dependent on the
10 secret information.

4. The system according to claim 1, wherein the anonymous signing section authorizes the individual data based on a group signature scheme.

5. The system according to claim 1, wherein the
15 anonymous signing section authorizes the individual data based on an escrowed identity scheme.

6. The system according to claim 1, wherein the anonymous signing section comprises:

a generator creating section for creating a
20 session-dependent generator depending on the session-related information;

00765390-04394
T002210-00255260

FQ5-511

34

a group signing section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by

5 raising the session-dependent generator to a power determined by the secret information; and

a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the

10 individual data and/or the session-related information.

7. The system according to claim 6, wherein the secret information is represented by (x, y, v) that satisfies: $v = (y + \delta)^{1/e} \bmod n$, where $y = a^x \bmod n$, n is a product of two prime numbers as used in the RSA cryptography, g is a generator that

15 generates a cyclic group of order n , a is an integer mutually prime to n , e is an integer mutually prime to the Euler number of n , and δ is a constant other than 1.

the generator creating section creates a session-dependent generator g_A corresponding to a session A

20 and a generator g_m is generated based on the individual data m and/or the session A .

the group signing section sets $z = g_A^x$ and generates a first proof statement

$$V_1 = \text{SKLOGLOG}(z, g_A, a) [\alpha: z = g_A^{(a^\alpha)}] (1)$$

FOLEY & LARDNER

FQ5-511

35

proving the knowledge of α satisfying $z = g_A(\alpha)$, and a second proof statement

$$V_2 = \text{SKROOTLOG}(z * g_A^b, g_A, e) [\beta: z * g_A^b = g_A(\beta^e)](1)$$

proving the knowledge of β satisfying $z * g_A^b = g_A(\beta^e)$,

- 5 the linkage data generating section sets $z_1 = g_m^y$,
and generates a third proof statement

$$V_3 = \text{SKREP}(z_1/z, g_m/g_A) [\gamma: z_1/z = (g_m/g_A)^\gamma](1)$$

proving the knowledge of z_1 and z have the same power to the bases g_m and g_A , respectively.

- 10 wherein the anonymous participation data is defined
as $(A, m, z, z_1, V_1, V_2, V_3)$.

8. The system according to claim 7, wherein

the anonymous signature determining section checks V_1 , V_2 , and V_3 of the anonymous participation data to determine
15 whether received data is anonymous participation data with
anonymous signature authorized by the participant subsystem,
and

- the sender match determining section checks z of the
anonymous participation data to determine whether anonymous
20 signatures of arbitrary two pieces of anonymous participation
data are signed by an identical participant subsystem.

9. The system according to claim 1, wherein the
anonymous signing section comprises:

FOLE & LARDNER

FQ5-511

36

a generator creating section for creating a generator depending on the session-related information;

a group signing section for signing the individual data using the generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information.

10. The system according to claim 9, wherein the secret information is represented by (x, y, v) that satisfies: $v = (y + \delta)^{1/e} \bmod n$, where $y = a^x \bmod n$, the individual data is denoted by m . n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n , a is an integer mutually prime to n , e is an integer mutually prime to the Euler number of n , and δ is a constant other than 1,

the generator creating section creates a session-dependent generator g_A corresponding to a session A .

the group signing section sets $z = g_A^x$ and generates a first proof statement

$$V_1 = \text{SKLOGLOG}(z, g_A, a) [\alpha: z = g_A^{(\alpha)}] (m)$$

proving the knowledge of α satisfying $z = g_A^{(\alpha)}$, and a second proof statement

$$V_2 = \text{SKROOTLOG}(z * g_A^{\delta}, g_A, e) [\beta: z * g_A^{\delta} = g_A^{(\beta^e)}] (m)$$

proving the knowledge of β satisfying $z * g_A^{\delta} = g_A^{(\beta^e)}$,

FQ5-511

37

wherein the anonymous participation data 13 is designated as (A, m, z, V_1, V_2) .

11. The system according to claim 10, wherein
the anonymous signature determining section checks
5 V_1 , and V_2 of the anonymous participation data to determine whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

the sender match determining section checks z of the
10 anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

12. The system according to claim 1, wherein the anonymous signing section comprises:

15 a generator creating section for creating a session-dependent generator depending on the session-related information;

an escrow identifying section for signing the individual data using the session-dependent generator and the
20 secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information; and

FOLE & LARDNER

FQ5-511

38

a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session-related information.

- 5 13. The system according to claim 12, wherein the secret information is represented by (a, b) that satisfies
- $b = (a^e - \delta)^{1/e} \bmod n$, where n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n , a is an integer mutually prime to
- 10 n , e is an integer mutually prime to the Euler number of n , and δ is a constant other than 1,

the generator creating section creates a session-dependent generator g_A corresponding to a session A and a generator g_m is generated based on the individual data

15 m and/or the session A ,

the escrow identifying section sets $z_a = g_A(a^e)$ and generates a first proof statement

$$V_1 = \text{SKROOTLOG}(z_a, g_A, e)[\alpha: z_a = g_A(a^e)](1)$$

proving the knowledge of α satisfying $z_a = g_A(a^e)$, and sets z_b

20 $= g_A(b^e)$ and generates a second proof statement

$$V_2 = \text{SKROOTLOG}(z_b, g_A, e)[\beta: z_b = g_A(b^e)](1)$$

proving the knowledge of β satisfying $z_b = g_A(b^e)$, and

the linkage data generating section sets $z_c = g_m(a^e)$ and generates a third proof statement

25 $V_3 = \text{SKREP}(z_c/z_a, g_m/g_A)[\gamma: z_c/z_a = (g_m/g_A)^\gamma](1)$

FOLEY & LARDNER

FQ5-511

39

proving the knowledge of z_a and z_c having the same power to the bases g_A and g_m , respectively,

wherein the anonymous participation data is defined as $(A, m, z_a, z_b, z_c, V_1, V_2, V_3)$.

5 14. The system according to claim 13, wherein
the anonymous signature determining section
determines whether $z_a/z_b = g_A^s$ is satisfied and checks V_1 , V_2 ,
and V_3 of the anonymous participation data to determine whether
received data is anonymous participation data with anonymous
10 signature authorized by the participant subsystem, and

the sender match determining section checks one of
 z_a and z_b of the anonymous participation data to determine
whether anonymous signatures of arbitrary two pieces of
anonymous participation data are signed by an identical
15 participant subsystem.

15. The system according to claim 1, wherein the
anonymous signing section comprises:

a generator creating section for creating a
session-dependent generator depending on the session-related
20 information; and

an escrow identifying section for signing the
individual data using the session-dependent generator and the
secret information to produce anonymous participation data,
wherein the anonymous participation data includes data

FOLETO-06E99260

FQ5-511

40

obtained by raising the session-dependent generator to a power determined by the secret information.

16. The system according to claim 15, wherein the secret information is represented by (a, b) that satisfies

5 $b = (a^e - \delta)^{1/e} \bmod n$, where n is a product of two prime numbers as used in the RSA cryptography, g is a generator that generates a cyclic group of order n , a is an integer mutually prime to n , e is an integer mutually prime to the Euler number of n , and δ is a constant other than 1,

10 the generator creating section creates a session-dependent generator g_A corresponding to a session A ,

the escrow identifying section sets $z_a = g_A(a^e)$ and generates a first proof statement

$$V_1 = \text{SKROOTLOG}(z_a, g_A, e)[\alpha: z_a = g_A(a^e)](m)$$

15 proving the knowledge of α satisfying $z_a = g_A(a^e)$, and sets $z_b = g_A(b^e)$ and generates a second proof statement

$$V_2 = \text{SKROOTLOG}(z_b, g_A, e)[\beta: z_b = g_A(b^e)](m)$$

proving the knowledge of β satisfying $z_b = g_A(b^e)$,

wherein the anonymous participation data is defined

20 as $(A, m, z_a, z_b, V_1, V_2)$.

17. The system according to claim 16, wherein

the anonymous signature determining section determines whether $z_a/z_b = g_A^b$ is satisfied and checks V_1 and V_2 of the anonymous participation data to determine whether

FOUO 00259260

FQ5-511

41

received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

the sender match determining section checks one of z_s and z_r of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

18. An anonymous participation authority management method for a system comprising:

10 a participant subsystem that is authorized to anonymously participate in a plurality of sessions using secret information; and

a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session.

the method comprising the steps of:

at the participant subsystem,

a) authorizing individual data using the secret information depending on session-related information to produce anonymous participation data with anonymous signature;

at the reception subsystem,

b) determining whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem; and

FOLE & LARDNER

FQ5-511

42

c) determining whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

19. The method according to claim 18, wherein the
5 anonymous signature includes data that is generated by a predetermined expression using the session-related information and the secret information, wherein the step (c) is performed by checking the data included in the anonymous signature of received anonymous participation data.

10 20. The method according to claim 19, wherein the predetermined expression is represented by raising a session-dependent base to a power that is dependent on the secret information.

21. The method according to claim 18, wherein the step
15 (a) comprises the steps of:

creating a session-dependent generator depending on the session-related information;

signing the individual data using the session-dependent generator and the secret information to produce
20 anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information; and

FOLE & LARDNER

43

22. The method according to claim 18, wherein the step (a) comprises the steps of:

signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information.

[illegible]